Mark Cyzyk. Book Review: Rolf Oppliger's *Internet and Intranet Security*, in *Telecommunications Electronic Reviews*, v5 (7), September 1998.

http://www.ala.org/ala/mgrps/divs/lita/ter/terv5n7september.cfm#oppliger

ter

telecommunications electronic reviews

Volume 5, Issue 7, September 1998

Telecommunications Electronic Reviews (TER) is a publication of the Library and Information Technology Association.

REVIEW OF: Rolf Oppliger. Internet and Intranet Security. Norwood, MA: Artech House, 1998.

by Mark Cyzyk

This is not a "how to" book; rather, it is a textbook on the state of the art in network security, specifically network security as it is currently implemented on the Internet and on local intranets. Lest the label "textbook" discourage readers however, I must point out that Oppliger's work is readable and informative for those seeking a detailed survey of the current architectures and protocols involved in securing information systems connected to the Internet or an intranet.

Oppliger begins by reviewing the nature of TCP/IP networking and the various network layers that are of key concern in securing an information system. He introduces something he calls the Internet Model, a simplification of the familiar Open System Interconnect (OSI) model, as a heuristic device to be used throughout the book. Instead of the seven layers of the OSI model, the Internet Model is

comprised of only four: The Network Layer, the Internet Layer, the Transport Layer, and the Application Layer. The book details the means of securing each of these network layers.

Before doing so, however, Oppliger provides a fine introduction to cryptographic techniques, authentication types, and key distribution including one-way hash functions, secret key cryptography, public key cryptography, password-based authentication, address-based authentication, cryptographic authentication, manual key distribution, center-based key distribution, and certificate-based key distribution. With this as a general background he then proceeds to a discussion of some specific security techniques as applied to each layer of the Internet Model.

The first type of technology Oppliger discusses is firewall technologies, and these are of two types: Packet filters and application gateways. Essentially, a packet filter is a firewall system that operates at the Internet Layer of the Internet Model. It examines each and every incoming packet and, following predetermined packet filtering rules, allows or disallows packets into an internal network. Packet filters can ensure that, for example, requests for various Internet services (telnet, SMTP) occur only on the common port numbers to which those services are normally bound. Moreover, a packet filter can combat IP spoofing by passing only those packets whose origin is from an IP address outside of the internal network. Thus if a hacker attempts to use an internal, trusted IP to gain access to the internal network from outside, the packet filter will determine that an internally-assigned IP is attempting to cross the firewall from an external network and will disallow it.

Whereas packet filters operate at the Internet Layer of the Internet Model, application gateways operate at the transport or application layers depending upon whether they are a circuit-level gateway or an application-level gateway, which Oppliger distinguishes and defines. In either case, an application gateway is a sort of proxy server for each application protocol being run on a network; if a network uses the telnet protocol, for example, there will exist a telnet daemon running as a proxy on an application server somewhere between the inside and outside networks that screens, logs, and performs other accounting functions on all telnet transactions attempting to cross. The same holds for other applications and protocols.

After an insightful discussion of firewall placement on a network, Oppliger proceeds to introduce and detail the various proposed and currently implemented Internet Layer communications protocols. These include: Security Protocol 3, Network Layer Security Protocol, Integrated NLSP, swIPe, IPv6, and several others. For those with an interest in low-level protocols, this should prove fascinating--for this reviewer, however, the level of detail was uninteresting. Nevertheless, such a discussion certainly belongs in a book of this type.

What was more interesting was Oppliger's next topic: Transport Layer Security Protocols. These include Security Protocol 4, Secure Shell, Private Communication Technology, and Secure Sockets Layer (SSL). The level of technical detail involved in Oppliger's elaboration of how SSL operates was interesting, perhaps because SSL is such a common, widely implemented protocol.

In his chapter on Application Layer Security Protocols, Oppliger broaches the topic of secured applications such as Secure Telnet, the various flavors of secure email systems, and Secure HTTP. His narrative on PGP-encrypted email and Secure MIME is surely a sign of things to come. These technologies are here now, but not commonly implemented. As email becomes more and more central to the inner workings of societies around the world, its security will quickly become of prime importance--and encrypted email systems will certainly become prevalent.

He concludes the book with a brief look at electronic commerce as well as a short survey of Internet security tools (e.g., Satan, COPS, TCP Wrapper). In all, the book provides a fine overview of the state of the art in Internet security. It was not, however, an easy read in places and is certainly not a book to be consulted for practical advice.

Mark Cyzyk (mcyzyk@towson.edu) is the University Webmaster at Towson University in Towson, Maryland. He was formerly the Head of Information Technology in the Albert S. Cook Library at Towson University.

About TER

Technology Electronic Reviews (TER) is an irregular electronic serial publication of the Library and Information Technology Association, a division of the American Library Association, 50 E. Huron St., Chicago, IL 60611. The primary function of TER is to provide reviews of and pointers to a variety of print and electronic resources about information technology. Resources include books, articles, serials, discussion lists, training materials, bibliographies, and other items of interest to librarians and information technology professionals. The topics covered may include, but are not limited to, networking technologies and standards; hardware and software; operating systems; databases; specific programming languages; management tools and utilities; technical project management; training and personnel issues; library perspectives; and research and development.

Opinions expressed in this publication are those of the writers and do not necessarily represent the viewpoints of LITA, ALA, or organizations involved in the storage and/or distribution of the publication.

TER is distributed electronically via Internet. There is no subscription fee. Currently it is available via World Wide Web (http://www.lita.org/ter/) and new-issue announcements are posted on the LITA-L electronic discussion list. To subscribe, send an email message to listproc@ala1.ala.org that says:

subscribe LITA-L First-Name Last-Name. Other distribution arrangements may be made in the future.